

SPECIFICATION AMENDMENTS

Please replace paragraph [0075] of the subject application with the following paragraph:

[0075] At periodic intervals, for example, the license authorities may update their respective shares of the private key SK through execution of the respective update module 222 of FIG. 2. At block 802, each license authority i generates a random (k, m) sharing of the secret 0 using a random update polynomial f_i , $update(X)$, as shown in Equation (9):

$$f_{i,update}(x) = b_{i,1}x + \dots + b_{i,k-1}x^{k-1} \bmod N \quad (9)$$